The empirical study on human flesh search based on neutralization theory

Wenli Li, Faculty of Management and Economics, Dalian University of Technology, Dalian, Liaoning, China, wlli@dlut.edu.cn

Na Wu, Faculty of Management and Economics, Dalian University of Technology, Dalian, Liaoning, China, wu_na880710@163.com

Yulong Ke, Faculty of Management and Economics, Dalian University of Technology, Dalian, Liaoning, China, keyulong@mail.dlut.edu.cn

Xin Lv, State Information Center, Beijing, China, lux@cei.gov.cn

Yulin An, Faculty of Management, Zhe Jiang University, Hangzhou, Zhejiang, China, leremyan93@gmail.com

Abstract

Human Flesh Search (HFS) is a search phenomenon emerging on the Internet in recent years, which integrates machine search and manual search, and is usually used to find or identify immoral events or characters. But problematically in the process of HFS, the personal information of search objects is posted on the Internet, which seriously violates the privacy protection of the search objects and affects the real lives of others. In this paper, we apply the neutralization technology theory and deterrence theory, both prominent in criminology, with the construction of privacy awareness, to study the behavior of participants of the HFS. Using smartPLS2.0 software to analyze 574 questionnaires, we got our research conclusion. We find that the technologies of denial of responsibility, denial of injury, denial of victim, appeal to higher loyalties, avoidance of greater harm and privacy awareness significantly influence the intention to participate in the HFS, but the metaphor of the ledger technology, the certainty of sanction and the severity of the sanction have no significant effect on HFS participation intention. Based on the results of this study, we conduct a detailed analysis and give some appropriate instructions. At last, the research conclusion may have some potentially fruitful reference for related legislation and be helpful to guide the Internet behavior of netizens.

Keywords: Human Flesh Search, neutralization technology theory, privacy awareness
1 INTRODUCTION

With the development of information technologies and the prosperity of virtual communities, online Human Flesh Search (HFS) is becoming an arising phenomenon which is spurred to become more powerful and affects our daily lives profoundly. “Human Flesh Search” which is named "cyber manhunt” in the West, is described as “A mass campaign, which comes into vogue through the medium of Internet, targeting at searching for the identity of a certain person or the truth about a certain event, whose data collection depends partially on the human force for filtering the information gained from the search engine, and partially on the anonymous or real-name information announcement.”(Wang et al. 2009) Although this phenomenon has been reported in many countries, most of the academic articles about HFS is concentrated in the Chinese context. Since the inception of HFS events during 2001 to 2010, a total of about 404 HFS episodes were reported(Wang et al. 2010). In 2008, there were 114 HFS episodes reported, among which 111 happened in China. In 2009, a total of 168 HFS episodes took place, including 163 in China, a rising trend was continued throughout 2009 and 2010(Wang et al. 2010). The purpose of HFS is to expose personal information details of a target whose action is a violation of the mainstream moral standard or incompatible with social justice (Cheng et al. 2012). Consequently, HFS involves serious misbehaviors such as privacy violation and even personal attack (Chao&Tao 2012).

Due to the interdisciplinary characteristic, HFS has attracted much research attentions from different academic fields. Most of them focus on the fields of legal, social psychology and ethics. From the legal perspective, there exists contradiction between citizens’ right to privacy, the right to know (Weng&Wang 2002) and the freedom of speech (Li&Yang 2003). Weng and Wang(2002) acknowledged that the way to coordinate the conflicts of privacy and right to know is to distinguish between different areas of the contradiction of privacy and right to know then treat them differently (Xiao 2001). For the conflicts between the privacy and the freedom of speech, Lei(2009) considered that in the process of HFS, leakage and spread of someone’s personal information have violated his privacy, regardless of the freedom of speech. But Mao(2009) thought that improper restrictions on freedom of speech for protecting citizens' privacy will pose a hazard to citizen's basic constitutional rights. There are also many studies from the aspect of social psychology. Cheng et al. (2012) deemed that citizens are often out of interest or curiosity to participate in HFS, and there exists "herd effect" so obviously that many people follow the HFS initiators blindly as sheep following the herd. Sproull and Kiesler(1991)had argued that the deindividuation which is characterized by fall after fall in the sense of self-awareness and self-regulation would easily emerge at the setting of anonymous use of computers and when people in groups produce more aggressive, deviant, anti-normative, or socially unacceptable behaviors. As a group usually involves scarcely any individual evaluation and no assignment of responsibility to individuals, there is less direct reinforcement or punishment (Guerin 2003). Therefore, the individual regards group action as a diffusion of responsibility that is indistinct or can disappear (Chao&Tao 2012).

Much of the existing researches are focused on the field of law and sociology, however empirical study based on the perspective of information security is parsimoniously developed. Chao and Tao (2012) call for more quantitative and empirical participators of HFS justifications and rationalizations for their misbehaviors. To bridge this gap, neutralization theory and deterrence theory are introduced to investigate online users HFS behavior, and an empirical study is applied to dig the psychological motivation of online HFS participants in order to offer a new insight into how online citizens justify their behavior. We argue that neutralization technologies should be taken into consideration as significant factors to understand the behavior motivation of the HFS participators as well as privacy security awareness of online users.
2 THEORY AND HYPOTHESIS DEVELOPMENT

2.1 Neutralization Theory

Proposed by Sykes and Matza (1957), the neutralization theory is a method for the violator to justify his unlawful acts and relieve the guilt (Priest&McGrath III 1970). The neutralization techniques can help them to form false appearance of innocence and switch between the unlawful and legal behaviors constantly.” It is our argument that much delinquency is based on what is essentially an unrecognized extension of defenses to crimes, in the form of justifications for deviance that are seen as valid by the delinquent but not by the legal system or society at large.” (Sykes&Matza 1957) Neutralization theory mainly consists of five techniques, including the denial of responsibility, denial of injury, denial of victim, condemn of the condemners and the appeal to higher loyalties (Sykes&Matza 1957). Afterwards, Garrett et al.(1989) expanded the techniques of neutralization theory and put forward a new technique, avoidance of greater harm, and Klockars (1974) came up with the technology of the metaphor of the ledger.

Neutralization theory has been widely applied in the research field of criminology. Eliason and Dodder(1999) applied the neutralization theory in studying the deer poachers, discovering that the denial of responsibility and condemn of the condemners were two neutralization techniques adopted by the deer poachers. In the studies on the drug abuse among the youngsters, Priest and McGrath III (1970) had showed that the neutralization techniques, including the denial of responsibility, the denial of injury, the denial of victim and the appeal to higher loyalties, were frequently taken by the drug abusers. Similarly, the tax evaders also exploited various neutralization techniques to defend themselves, which largely decreased their sense of guilt (Thurman et al. 1984). Although Sykes and Matza (1957) deemed that the neutralization theory could only be applied in the criminology field, the subsequent substantial researches had confirmed that this theory also had good explanation in other fields (Pershing 2003). Akerst(1999) discovered that the criminology theory could not only be applied for explaining the illegal behaviors, but also accounted for any legal behaviors that violated the social rules. In the area of the IS (information system), according to the studies about pirated products, appeal to higher loyalties technique was used by the people who may use the both pirated software and pirated music, while the denial of responsibility, denial of injury and denial of victim techniques were prevalent in pirated music users’ justifications (Ingram&Hinduja 2008), and the condemn of the condemners technique was used to justify pirated software use(Siponen et al. 2010). Harrington (1996) found that the relationship between the denial of responsibility and the computer abuse intention was significant, and the computer abuser did not regard it as illegal behavior. Siponen and Vance (2010) showed that the neutralization theory significantly influenced the employees’ intention to violate the enterprise information security system, and the existence of the neutralization technologies may undermine the effect of the deterrents.

In the research context of HFS, we argue that neutralization theory can effectively excavate the psychological process of the online citizens participating in the HFS. Denial of responsibility, denial of injury, denial of victim and appeal to higher loyalties are adopted from Sykes and Matza (1957), avoidance of greater harm from Garrett et al. (1989), and metaphor of the ledger from Klockars (1974). Condemning of condemners is omitted for the reason that it is difficult to define who the condemnor was in the research context of this paper. Previous researches also suggest that the omission is not problematic.

2.1.1 Denial of Responsibility (DR)

Denial of responsibility refers to persons committing deviant acts define themselves as no need to be responsible for their misconducts (Rogers&Buffalo 1974; Sykes&Matza 1957). In other words, the violators transfer the accusation to others (Thurman et al. 1984), or claim that the illegal act is an inadvertent accident (Priest&McGrath III 1970). The delinquents argue that the action in question happens out of their control, so they don’t have to be responsible for it. As one of the neutralization
techniques, the denial of responsibility was always taken as some practical excuses, for instance the unlawful act was forced by the environment, the parents didn’t get along with each other, the colleagues were not so good (Siponen&Vance 2010). In the information system security policy context, Puhakainen and Ahonen (2006) reported that employees failed to comply with the company policy to encrypt confidential e-mails because the policy was indistinct. The denial of responsibility actually separates the individual from his behavior (Siponen&Vance 2010). When it comes to HFS, the actor disclosing other’s information might neutralize his behavior by claiming that he does not know it is illegal or how the rule stipulates. Therefore, the following hypothesis is proposed:

H1: Denial of responsibility positively affects intention to participate in HFS.

2.1.2 Denial of Injury (DI)

The denial of injury refers to the behavior of minimizing the injury brought by the unlawful act and rationalizing it(Thurman et al. 1984). The violators do not admit that their behavior caused any injury. In other words, the violators deny that their behavior is harmful, for no one is injured or there is no loss (Piquero et al. 2005). This technique may focus on the injury caused by the unlawful acts, and the violators think that their illegal actions can be forgiven since no one get hurt (Priest&McGrath III 1970). For instance, a car thief says that he ‘borrows the car’ and does not hurt anyone(Sykes&Matza 1957); many cheaters in the exam consider that it’s a mere trifle, and no one would be hurt(McCabe 1992) ; an employee deems that violation of the information security policies is no problem if there is no harm to the company(Siponen&Vance 2010). The denial of injury actually separates the individual behavior from its results (Siponen&Vance 2010). Under the context of HFS, the participants might claim that no harm is done to the society, as they do not attack the network to achieve the user’s information, just collect some of the user’s privacy information. Therefore, the following hypothesis can be proposed:

H2: Denial of injury positively affects intention to participate in HFS.

2.1.3 Denial of Victim (DV)

Even though the misfeasors admit that their behaviors may involve some injury and are willing to take the responsibility for their deviant actions, the moral outrage from themselves may neutralize their inappropriate behaviors in light of the circumstance (Sykes&Matza 1957). They may deny the existence of the victims, and then turn the victims to be the ones deserve the injury. Through delicate changes, the delinquents turn to the position of revengers, while the victims are transformed into the wrongdoers (Sykes&Matza 1957). The violators regard their behaviors as proper punishment for the victims (Priest&McGrath III 1970). Venting the dissatisfaction with the teachers or school leaders by destroying the public properties, stealing the products from the store of ‘bad shopkeeper’—in the eyes of these misbehaving people the victims should be punished (Sykes&Matza 1957). In another case, the victim may be an inexisten, unknown or abstract thing (such as reputation, etc.), and the awareness about the existence of the victim will decrease greatly (Siponen et al. 2010). For HFS, the partakers assert that the ones whose privacy is disclosed are immoral or inaccurate, and they deserve to be punished. Therefore, the following hypothesis is proposed:

H3: Denial of victim positively affects intention to participate in HFS.

2.1.4 Avoidance of Greater Harm (AGH)

The violator behaves unlawfully to avoid the occurrence of more similar injuries (Garrett et al. 1989). There will be more injuries if the victims who have served the devil are indulged continuously (Cody&McLaughlin 1985). For instance, the supermarket manager would claim that they change the products for avoiding unnecessary misunderstandings about the products next time, and the aim is nothing but promoting the things to develop towards good directions (Garrett et al. 1989). Under the context of HFS, this technique may explain the illegal behaviors better. For instance, if the addiction
in abusing cats is not disclosed, it will certainly result that more cats will be abused, and it aims to prevent the cat abuser from conducting more and severer things. Therefore, the following hypothesis is proposed:

\textit{H4: Avoidance of greater harm positively affects intention to participate in HFS.}

\textbf{2.1.5} \textit{Appeals to Higher Loyalties (AHL)}

Sometime, the delinquents aren’t willing to violate the established social rules, but they are in a dilemma and they have to appeal to higher loyalty at the risk of violating the established rules. They run counter to certain norms not because the rules themselves are inappropriate, but because they have no choice but to obey the higher-level and more authoritative rules (Sykes&Matza 1957). The delinquents don’t abide by the general rules but the rules for the special group. In their eyes, the group rules are prior to the general rules; as a result, they will obey the former and violate the latter (Piquero et al. 2005). For instance, the employees may claim that they have to infringe the company clause to accomplish the work arranged by the manager (Siponen&Iivari 2006). The conflict between the friendship and law has already been realized as a common problem by the social scientists. Put into the dilemma between the friendship and law, the youth offenders are finally turned to be culprits for insisting on the belief ‘they have to help their friends out of difficulty’ and ‘never sell your buddies’ (Sykes&Matza 1957). The young drug abusers worry that their friends may feel disappointed if they don’t take the drugs, and they may even lose friends (Priest&McGrath III 1970). Under the context of HFS, many citizens participate in the HFS for the sake of justice and social morality. Pan(2010) asserted that one of the factors motivating participation in HFS was contribution to justice. Therefore, the following hypothesis is proposed:

\textit{H5: Appeal to higher loyalties positively affects intention to participate in HFS.}

\textbf{2.1.6} \textit{The Metaphor of the Ledger (ML)}

The metaphor of the ledger means to use good actions to compensate for bad acts(Klockars 1974). In other words, an individual believes that he/she can afford to do some bad actions because of his or her good acts before (Klockars 1974). It reduces the criminals’ guilty feelings by allowing them to view their deviance as unrepresentative of overall good nature (Thurman et al. 1984). For example, Dabney (1995) studied the metaphor of the ledger in a hospital context and found that the nurses always excused themselves that they observed the “fringe benefit” to neutralize their theft of supplies and over-the-counter medicines (Dabney 1995). Lim (2002) observed that employees felt no guilty for their surfing the Internet for personal issues during working because of their good job performance. Siponen and Vance (2010) argued that employees neutralize their occasional violation of security policies through their general adherence to them. In the eyes of the HFS participation, their behaviors can be compensated by their obeying to laws in real life or good online performance before. Therefore, the following hypothesis is proposed:

\textit{H6: The metaphor of the ledger positively affects intention to participate in HFS.}

\textbf{2.2} \textit{Privacy Awareness (PA)}

In the information security field, the information security awareness in the organizational environment refers to the employees’ attention to the information security and the understanding about information security requirements in the organization (Choi et al. 2008). Bulgurcu et al.(2009) discovered that the information security awareness can effectively enhance the employees’ intention to comply with the information security system. Siponen (2000) once analyzed the information security awareness conceptually and proposed some measures to strengthen the awareness from the theoretical perspectives. Soon afterwards, Hentea(2005) strengthened the significance of information security awareness education and training in real life, pointed out the shortages of the current educational method from various aspects and proposed targeted improvement method. Goodhue and Straub (1991)
argued that the awareness is a significant factor in constructing one’s belief in information security. Similarly, Siponen(2001) also thought that, any use of the Internet equipment as long as directly or indirectly under the Internet context, the consciousness should be taken into consideration. We introduced the constructs of privacy awareness in the research context because of considering about the significance of privacy awareness and its relevance to the participation intention.

The concept of privacy awareness has been mentioned by a lot of articles. Some scholars put forward the privacy awareness system from the perspective of ubiquitous computing, while some scholars remind the netizens to improve the privacy awareness from the perspective of social network; Phelps et al.(2000) thought that privacy awareness refers to the individual’s understanding and the extent to which an individual is informed about the organizational privacy operations. Later in 2009, Pötzsch(2009) determined a more detailed definition of privacy awareness, which comprised attention, perception and cognition of: (1) Whether others have received personal information about him/her, his/her presence and activities; (2) How these pieces of information are processed and used; (3) What amount of information about the presence and activities of others might reach and/or interrupt the individual.

At the setting of HFS, we take the point of view that the privacy awareness contains two layers of meaning for the network users: (1) Firstly, individuals should have clear cognition about self-privacy information and appropriate measures should be taken to protect the self-privacy information, what is the right of citizens; (2) Secondly, citizens should explicitly define other’s privacy information and understand the results of disclosing others’ privacy information, what is the obligations of citizens. From the perspective of offenders, the privacy awareness mainly focuses on the latter. The participants of HFS reflect low sense of privacy awareness. They have unclear understanding or cognitive error about the consequences of reveal others’ privacy. The lower privacy awareness the citizens have, the higher possibility to take part in the activities for HFS. Therefore, the following hypothesis is proposed:

H7: Privacy awareness negatively affects intention to participate in HFS.

2.3 Deterrence Theory

To gain abidance by the law, the criminal justice system seeks out individuals who conducts illegal actions and implement punishment for these acts (Tyler&Hu02). The threat of detection and punishment stops individuals from committing crimes. In order to examine whether an individual will be prevented from committing a criminal act, deterrence theory presents two factors: the perceived certainty of sanction (PC) and the perceived severity of sanction (PS) (Wolfie et al. 2008). The greater certainty and severity of the sanction is perceived, the lower possibility to commit criminals (Hovav&D’Arcy 2011). D’Arcy et al. (2009) developed an extended deterrence model and it predicted that perceived certainty and severity of organizational sanctions influence individuals’ IS misuse intention. In this study, certainty of sanctions refers to the probability of being punished, and severity of sanctions refers to the degree of punishment associated with engaging in the HFS. We expect that if the citizens perceive the chances of their participation in the HFS being detected is high, and the punishment is serious, their intention to participate in HFS is likely to decrease. Therefore, the following hypothesis is proposed:

H8: Perceived certainty of sanction negatively affects intention to participate in HFS.
H9: Perceived severity of sanction negatively affects intention to participate in HFS.

Therefore, the model is shown in figure 1:
3 METHOD

3.1 Measurement Items

In this study, questionnaire method was adopted for the data acquisition, which has been widely applied and recognized in the research field of IS security (Choi et al. 2008; Siponen&Vance 2010). The questionnaire was designed with hypothetical scenario method. The advantage of employing the hypothetical scenario method is that it can narrate the HFS events as the third person and in neutral language (Siponen&Vance 2010). Four representative HFS incidents had been showed in this study: (1). Liaoning girl¹; (2). Crushing Cats²; (3). Qian Jun Incident³; (4). Tong Xu Men⁴. The questionnaires consisted of three parts: The first part included 6 questions about basic information; the second part was the scenario investigation about the intention to participate in the HFS with 8 questions; the factor investigation for the neutralization theory and deterrence theory were measured in the third part with 29 questions. The second and third parts of the questionnaire were measured respectively with multiple items on seven-point Likert scales. In order to prevent the semantic problems in the questionnaires, 50 postgraduates from the information security research field were invited to pretest the questionnaires.

3.2 Data Collection

The questionnaires were mainly distributed in two ways, paper questionnaire and electronic questionnaire. The paper questionnaires were geared to the college students. The electronic questionnaires were issued through the questionnaire-star website and filled by citizens from all over the country. In this study, 500 paper questionnaires were sent and 400 of them were collected, with 330 electronic questionnaires back. After discarding a few questionnaires with incomplete answers or unreliable ones, about 574 valid questionnaires were obtained and the sample effective response rate

¹See : http://baike.baidu.com/view/2140375.htm
²See : http://baike.baidu.com/view/2506880.htm
³See : http://baike.baidu.com/view/2884820.htm
⁴See : http://baike.baidu.com/view/1105255.htm
was about 79%. In the final sample, 56% of the respondents were male, 63% have a degree of bachelor, and 74% were in the 21-30 age range. The statistics of the samples is shown in Table 1.

<table>
<thead>
<tr>
<th>Item</th>
<th>Variable</th>
<th>Frequency</th>
<th>Proportion</th>
<th>Item</th>
<th>Variable</th>
<th>Frequency</th>
<th>Proportion</th>
</tr>
</thead>
<tbody>
<tr>
<td>Gender</td>
<td>Male</td>
<td>323</td>
<td>56%</td>
<td>Current condition</td>
<td>Students</td>
<td>453</td>
<td>79%</td>
</tr>
<tr>
<td></td>
<td>Female</td>
<td>251</td>
<td>44%</td>
<td></td>
<td>Non-students</td>
<td>121</td>
<td>21%</td>
</tr>
<tr>
<td>Age</td>
<td>&lt; 20</td>
<td>121</td>
<td>21%</td>
<td>Major</td>
<td>Management information system or computer science</td>
<td>328</td>
<td>57%</td>
</tr>
<tr>
<td></td>
<td>21-30</td>
<td>424</td>
<td>74%</td>
<td></td>
<td>Other majors</td>
<td>245</td>
<td>43%</td>
</tr>
<tr>
<td></td>
<td>31-40</td>
<td>20</td>
<td>3%</td>
<td>Seldom using</td>
<td></td>
<td>3</td>
<td>1%</td>
</tr>
<tr>
<td></td>
<td>&gt; 41</td>
<td>9</td>
<td>2%</td>
<td>Time of using computer</td>
<td>1-3 hours</td>
<td>101</td>
<td>18%</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>4-6 hours</td>
<td>218</td>
<td>38%</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>7-10 hours</td>
<td>168</td>
<td>29%</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>More than 11 hours</td>
<td>84</td>
<td>15%</td>
</tr>
<tr>
<td>Education background</td>
<td>Junior degrees or bellow</td>
<td>87</td>
<td>15%</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Bachelor</td>
<td>364</td>
<td>63%</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Master or above</td>
<td>123</td>
<td>21%</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Table 1. Sample distribution

4 DATA ANALYSES AND RESULTS

4.1 Measurement Model

Smart PLS 2.0 (Ringle et al. 2005) was adopted to conduct the test of convergent validity, discriminant validity and reliability for the theoretical model which was used to assess the reliability and validity of the reflective scales. For convergent validity, which measures the degree to which the multi-items measures the same construct agree, it should meet the condition that all factor loadings should be above 0.7 threshold and average variance extracted (AVE) for each construct should be greater than 0.5 (Gefen & Straub 2005). As shown in Table 3, both criteria are met and therefore the convergent validity of all scales was adequate. Discriminant validity means the degree to which a construct is distinguished from the others. When the square root of the AVE of each construct is greater than the inter-construct correlation coefficient and all the AVE is greater than 0.5, it suggested that there is good discriminant validity among each construct (Gefen & Straub 2005). As seen in Table 2 and Table 3, both criteria are met and therefore the discriminant validity of all scales was adequate. Construct reliability is the degree to which items are got rid of random error, and generate similar scores (Gefen & Straub 2005). The composite reliability of each construct is above the acceptable level 0.7, and the Cronbach’s Alpha is greater than 0.8, which indicated that there is a good internal consistency in the scale, so the scale has high reliability. The result of constructs reliability is shown in Table 3.

<table>
<thead>
<tr>
<th></th>
<th>PC</th>
<th>PS</th>
<th>DI</th>
<th>DV</th>
<th>DR</th>
<th>AHL</th>
<th>ML</th>
<th>PA</th>
<th>INT</th>
<th>AGH</th>
</tr>
</thead>
<tbody>
<tr>
<td>PC</td>
<td>0.81</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>PS</td>
<td>0.76</td>
<td>0.85</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>DI</td>
<td>-0.28</td>
<td>-0.23</td>
<td>0.93</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>DV</td>
<td>-0.24</td>
<td>-0.27</td>
<td>0.61</td>
<td>0.93</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Table 2. Correlation of the Latent Variable Scores

<table>
<thead>
<tr>
<th>Constructs</th>
<th>DR</th>
<th>AHL</th>
<th>ML</th>
<th>PA</th>
<th>INT</th>
<th>AGH</th>
</tr>
</thead>
<tbody>
<tr>
<td>DR</td>
<td>-0.21</td>
<td>-0.27</td>
<td>-0.26</td>
<td>0.48</td>
<td>-0.29</td>
<td>-0.23</td>
</tr>
<tr>
<td>AHL</td>
<td>-0.21</td>
<td>-0.33</td>
<td>-0.25</td>
<td>0.57</td>
<td>0.62</td>
<td>0.47</td>
</tr>
<tr>
<td>ML</td>
<td>0.67</td>
<td>0.57</td>
<td>0.64</td>
<td>-0.34</td>
<td>0.62</td>
<td>0.74</td>
</tr>
<tr>
<td>PA</td>
<td>0.70</td>
<td>0.75</td>
<td>0.67</td>
<td>-0.34</td>
<td>0.66</td>
<td>0.79</td>
</tr>
<tr>
<td>INT</td>
<td>0.93</td>
<td>0.92</td>
<td>0.95</td>
<td>0.82</td>
<td>0.98</td>
<td>0.95</td>
</tr>
</tbody>
</table>

Table 3. Validity and Reliability of Reflective Construction

4.2 Structural Model

Figure 2 shows the results of model testing. About 60% of variance in intention to leak others privacy is explained by the model which indicates a robust explaining power for this model. Meanwhile, the path from denial of responsibility (H1: β=0.22, p<0.001), denial of injury (H2: β=0.17, p<0.01), denial of victim (H3: β=0.16, p<0.01), avoidance of greater harm (H4: β=0.14, p<0.05), appeal to higher loyalty (H5: β=0.12, p<0.05), privacy awareness (H7: β=0.10, p<0.01) to the intention to leak others privacy are significant. Therefore, we find support for H1, H2, H3, H4, H5 and H7. Whereas, the path for metaphor of the ledger (H6: β=0.04, p>0.05), perceived certainty of sanctions (H8: β=0.02, p>0.05), perceived severity of sanctions (H9: β=0.02, p>0.05) to the intention to leak others privacy are not significant which indicates H7, H8 and H9 are not supported.
Notes: *P<0.05; **P<0.01; ***P<0.001; N.S=not significant

Figure 2. PLS results of model testing

5 DISCUSSION, IMPLICATION AND LIMITATION

5.1 Discussion

Our study examined the participation of the HFS by netizens from the combined perspectives offered by neutralization, deterrence theory and privacy awareness. We find that privacy awareness and neutralization techniques except the technology of metaphor of the ledger are excellent antecedents of netizens’ intention to take part in the HFS, whereas the two dimensions of formal deterrence do not influence the netizens’ intention to participate in HFS. Based on our empirical results, there are three findings we need to highlight. The first finding is that our results provide encouraging evidence which suggests that neutralization theory may be useful in shedding light on the reason why HFS continues to be a pervasive problem in China. This finding is consistent with neutralization studies in other domain. To date, neutralization techniques have been used to explain poaching behavior (Eliaison&Dodder 1999), deviant actions in a military environment (Pershing 2003), corporate crime (Piquero et al. 2005), and so on. In IS security, many studies, as computer abuse study (Harrington 1996), cyberloafing study (Lim 2002), software piracy (Hinduja 2007) and IS violation (Siponen&Vance 2010) also employ a portion of neutralization technologies to explain inappropriate behaviors in organizations. In our study, the technologies of denial of responsibility, denial of injury, denial of victims, avoidance of greater harm, and appeal to higher loyalties have significant influence on HFS participation, which are new predictors of HFS participation. It is particularly worth mentioning here that the technology of avoid of greater hurts had not been applied to other areas since it was firstly proposed by Garrett et al.(1989), had a significant influence on the behavior intention. So the successful application of the theory is one of the contributions of our study.

Secondly, the effect of certain of sanction and the severity of sanction on intention to participate in HFS is insignificant. There may be two reasons for it. On the one hand, the neutralization maybe a factor what reduces the influence of deterrence, which is the same as Siponene' (2010) conclusion that the existence of neutralization technology may lead deterrence effect to be a failure. Harrington(1996) also found the effect of rationalizing is so strong that the effects of codes of ethics, a kind of deterrence, become comparatively weak. On the other hand, current penalties for participants in the HFS are not clear, as a result netizens may have no sense of the threat of punishment. In other words, they do not know they may get punished if they engage in the HFS.

Thirdly, this is the first time to propose privacy awareness as a construct separately in the field of HFS, and according to our empirical result, the privacy awareness is a significant factor to influence the netizens’ intention to participate in the HFS. Despite the importance of information privacy awareness, there is a paucity of empirical studies that analyze the impact of information privacy awareness on information security domain. Bulgurcu(2010) studied the direct and indirect roles of information security awareness on an employee’s compliance behavior. D’Arcy et al. (2009) suggested that there are three security countermeasures can be employed to reduce employees’ IS misuse, which are user awareness of security policies; security education, training, and awareness (SETA) programs; and computer monitoring. In our study, we successfully proved that privacy awareness is an important factor and we need to pay more attention to it.

5.2 Implications for Research Practice

One of the primary objectives of our research was to inspect which neutralization techniques have strong influence on the participation of HFS. Denial of responsibility, denial of injury, denial of victim, avoid of greater hurts, appeal to higher loyalty are obviously increases the netizens’ intention to participate the HFS. On the one hand, they do not think that they should undertake the legal
responsibility after participate the HFS. Instead, they blame it to the unsound law system. They do not take care of the damage to the victims, and they claim that the victims deserve it because of their deviant behaviors. On the other hand, the participators judge their behaviors through some excuse, for example, they are firmly convinced that if they do not take some actions to prevent the deviant behavior, more damage will occur; they take part in the HFS or leak someone’s privacy information for the purpose of maintaining justice and protecting the weak. Based on the empirical findings, we summarize the following strategies to fight with the neutralization technologies netizens employed. From the analysis above, we can draw some reality enlightenment and should take emergency measures to resist the neutralization. From the perspective of the government, the improvement process of the privacy laws and rules should be accelerated and extensive dissemination of privacy laws and administrative regulations are needed. There must be laws to go by, the laws must be observed and strictly enforced, and lawbreakers must be prosecuted. In addition, the government also should strengthen the supervision of network public opinion, positively guide civilized Internet behavior, and purify the public opinion platform.

From the point of view of mass media, they should be able to identify what information can be spread, and what cannot. As privacy spreading channels and medium, mass media and the Internet companies should strengthen their own professional ethics and social responsibility, correctly guide public opinion towards rationalization.

Last but not the least, we individuals should pay attention to from the following several aspects: firstly, netizens should realize that everyone has to take the responsibility for the consequence of his behavior, rather than only regard himself as the victim of the social environment. Secondly, people need to strengthen their idea of rule by law, anyone has no right also is banned to infringe upon others privacy. Thirdly, if netizens find deviant actions, they should report them to relevant departments, rather than presumptuously uploaded to the network or leak others' privacy. Fourthly, in this study, we found that privacy awareness significantly influence the HFS participation intention. Based on this, we come up with some ways to improve the netizens’ privacy awareness. As for the students, the information security courses or lectures should be offered to improve the students’ information privacy awareness. For the employees, we suggest that the corporations establish training sessions or other meetings where the employees are persuaded to understand the importance of the privacy awareness. Besides, the managers or supervisors should be encouraged to raise their privacy awareness because the influence of leadership has been reported as a promising avenue to increase security policy compliance (Choi et al. 2008). As for the general netizens, the advertising films or other publicity means can be adopted to improve their privacy awareness.

5.3 Limitations

This study is subject to typical limitations, which stems from the use of intention as the dependent variable. We use two arguments from the previous literatures to response to the question whether the intention indicates actual behavior. Firstly, in the criminological research, there are many studies measuring the intention as a motivation state or predisposition to commit an act and are widely accepted (Siponen et al. 2010). Secondly, available literatures have proved that the relationship between intention and behavior is very firm (Fishbein&Ajzen 1975; Green 1989). In conclusion, although we did not measure the netizens’ actual behavior, the use of scenario-based intention can be more conducive to measure real ideas.

6 CONCLUSION

In this paper, the techniques of neutralization theory and deterrence theory are applied in the studies about the influence factors of the HFS participation intention, the findings suggest that neutralization theory can be a useful framework for understanding the participation of HFS and bear important policy and theoretical implications for efforts to address this behavior. Additional, the certainty and severity of the sanction could not deter the netizens to give up HFS, but the improvement of privacy
awareness can be a supplement to help to decrease the intention to take part in the HFS. Based on the findings above, some management implications have been proposed. Firstly, it is urgent for the government to make relevant laws about privacy in China with forceful publicity, so that people can learn that there are laws and stipulation to abide by. Secondly, for the mass media, they should strengthen their own professional ethics and social responsibility. Lastly, the general netizens should improve their privacy awareness, and acknowledge that there is no excuse to neutralize their deviant actions. This theoretical model has explained the influence factors for 60% of the HFS participating intention. And there are still many other factors that have not be found yet. In the future studies, we will be devoted to exploring other influence factors to perfect the current model.

References:

and courts, Russell Sage Foundation Publications.


